REMARKS/ARGUMENTS

The Examiner objected to the oath and declaration. Applicants have submitted a new oath in accordance with the Examiner's instructions.

The Examiner further objected to the title, abstract and portions of the specification. Applicants have amended the foregoing sections pursuant to the Examiner's comments.

Claims 1-22 remain in this application. Applicants canceled claims 23-49 to remove the double patenting rejection related to co-pending Application No. 10/238,950 (the '950 application"). Applicants will pursue claims 23-49 in the '950 application and address the corresponding rejections in that case.

§112, 2nd Paragraph

The Examiner rejected claims 1-22 under 35 U.S.C. §§112, 2nd paragraph due to informalities. In response to the rejection, Applicants have amended the claims pursuant to the Examiner's instruction by deleting the term "numbered" in claim 1 and all future recitations and by deleting the term "the number on" in claim 1 and all future recitations.

For these reasons, Applicants assert that the §112 rejections have been overcome.

§102 Rejections

The Examiner rejected claims 1-5, 7, and 14-21 under 35 U.S.C. §102(e), as being anticipated by U.S. Patent No. 6,424,954 of Leon ("Leon1"). For at least the reasons stated below, Applicants assert that all of the foregoing claims are allowable over Leon1.

Leon1 does **not** teach an indicium or postage stamp that comprises a "nonce", as set forth in the amended claims, which is used to generate a digital certificate. Independent claim 1 recites the use of a nonce stamp including a "nonce", and a digital certificate that is

securely derived from the nonce. The "nonce" element has been amended to clarify that the nonce comprises a "relatively unique number that substantially prevents a single user from accumulating multiple nonce stamps bearing the same nonce." This amendment and its distinction over the prior art of reference were discussed in an interview with the Examiner on April 19, 2004.

Support for this amendment is found in the pending application at page 6. Particularly, Applicants explain the terms "nonce stamp" and "nonce" as follows:

> The term "nonce stamp" is used herein to denote a physical article that is relatively difficult to copy illicitly (or equivalently, for which forgeries are easily detected and are preferably traceable) -- such as a typical postage stamp, for example -- and that also bears a "nonce." ... **In the context of the present invention, "nonce" denotes a number (or other datum) chosen from a good enough distribution to ensure relative "uniqueness," i.e., a low likelihood that a single user/customer can accumulate multiple nonce stamps bearing the same nonce number.**

(Emphasis added). Thus, Applicants have amended the term nonce to correspond to the above-referenced definition. The purpose of this "nonce" is to ensure security of the digital certificate, i.e., to ensure that illicit copies cannot be made of a digital certificate corresponding to a nonce and used with multiple nonce stamps bearing the nonce. (Pending application at page 10, line 26 - page 11, line 1).

Leon1 fails to disclose or suggest the use of a nonce stamp bearing a nonce having a relatively unique number, i.e., a number that is unique enough to substantially prevent a single user from accumulating multiple nonce stamps with the same number. With respect to Leon1, the Examiner argues that the "device ID and time of creation" read on the claimed nonce. However, such an interpretation would contradict the definition of "nonce" as set forth in the specification and explicitly recited in the amended claim. That is, by allowing a device ID and time or creation (i.e., a time stamp) to serve as a nonce, many different nonce stamps could be issued from the same metering device would have the exact same nonce. Clearly, the device ID number of a device will not change over the life of the device. Therefore, all stamps issue from the same metering device will bear the same device ID number. This number is therefore not "relatively unique" as defined by the claim, since a single user could accumulate many stamps having the exact same device ID number (i.e.,

every stamp printed by that metering device). Furthermore, the time of creation or "time stamp" will not provide a relatively unique number. For example, even if the "time of creation" indicia or stamp were accurate to one second, many nonce stamps could be printed out (e.g., using one or more high speed printers) that would bear the same time stamp. That is, many nonce stamps could be printed out within one second from a printer or from multiple printers (i.e., printer 152 and printer 170), as disclosed in Leon 1. Assuming the nonce stamps originated from the same metering device, they would also bear the exact same device ID. Therefore, all such postage issued during a particular time frame from the same metering device would bear an identical nonce (e.g., time stamp and device ID number). In this manner, a user could accumulate multiple stamps from the same metering device that would bear the same time stamp. The user could then derive a digital certificate from the nonce of one stamp and illicitly copy it over and over on all stamps bearing the same nonce. Therefore, neither the device ID, the time of creation, nor the combination of both can be construed to meet the nonce set forth in the amended claims.

Leon1 does not disclose or suggest the claim elements of a "nonce stamp" including a "nonce" comprising a relatively unique number that substantially prevents a single user from accumulating multiple nonce stamps bearing the same nonce. For at least these reasons, Leon1 cannot anticipate independent claim 1, or any claims depending from claim 1 (e.g., claims 2-5, 7 and 14-21). Therefore, Applicants respectfully request that the rejections of these claims on the basis of Leon1 be withdrawn.

§103 Rejections

The Examiner rejected claims 6, 8-13 and 22 under 35 U.S.C. §103. Particularly, the Examiner rejected claims 6 and 22 as being unpatentable in view of Leon1 in view of Ogg, and rejected claims 8-13 as being unpatentable over Leon1 in view of U.S. Pat. App. 2201/0042052 of Leon ("Leon2").

Leon1 in view of Ogg – claims 6 and 22

The Examiner argues that the combination of Leon1 in view of Ogg would render obvious claims 6 and 22. The Examiner relies on Ogg solely for its disclosure of a hashing

algorithm and the use of cryptographic techniques on any value-bearing item, such as tickets. For a proposed combination to render a claim obvious, it must teach or suggest *all* claim limitations. For at least all of the reasons set forth above, neither Leon1 nor Ogg provides any disclosure or suggestion regarding the claimed nonce stamp bearing a "nonce" comprising a "relatively unique number that substantially prevents a single user from accumulating multiple nonce stamps bearing the same nonce." Since neither Leon1 nor Ogg discloses or suggests these claimed limitations, the proposed combination cannot render obvious claims 6 and 22, which depend from independent claim 1. Therefore, Applicants respectfully request that the rejection of this claim on the basis of Leon1 and Ogg be withdrawn.

Leon1 in view of Leon2 – claims 8-13

The combination of Leon1 and Leon2 cannot invalidate any of the pending claims, as neither reference nor a combination of the two teach the unique and efficient system and indicium that uses a nonce stamp bearing a nonce (including a "relatively unique" number as defined in the claims) and a digital certificate derived from the nonce to authenticate a transaction, and since there is no motivation or suggestion to combine the references in the unusual way proposed by the Examiner.

In support of this rejection, the Examiner relies on Leon1 for the disclosure of a bar code and Leon2 for the disclosure of a serial number that may be used for security. Essentially, the Examiner argues that because one reference discloses an item bearing a serial number, it would be obvious to use the serial number as a nonce, to derive a digital certificate using the nonce, then to decode the digital certificate, and finally to compare the nonce to the digital certificate to authenticate the transaction. This argument is untenable as it contradicts the teachings of both Leon1 and Leon2, and since there is no suggestion or motivation to combine the two references in this unusual manner.

Leon1 teaches the use of a special metering device with special printing capabilities to allow pieces of mail to be authenticated. Specifically, in order to prevent counterfeits, Leon1 teaches using a securing metering device that can produce a "micro printing portion 916 that includes, for example, texts printed in small size fonts that are difficult to reproduce (i.e.,

using conventional printers)." (Leon1, column 40, line 23 – column 41, line 5). Furthermore, Leon1 teaches that this specialized device print a "fluorescent identifier" including "one or more elements for the purpose of identifying the indicium." (Id.) The ink used can include "taggants" or "microscopic identifiers" that allow for "analysis of an indicium to determine whether it originates form an authorized metering device." (Id.) The entire thrust of Leon1 is to provide a specialized metering device capable of generating several complex elements within the indicium that are nearly impossible to duplicate, and then to use another specialized device to detect these complex elements and verify the postage.

Thus, Leon1 uses a highly specialized metering device to create complex markings that cannot be duplicated and can only be read by other specialized machines in order to authenticate postage. As a result, there is no suggestion, necessity or motivation in Leon1 to employ Applicants' unique nonce, derive a digital certificate from the nonce, and compare the certificate to the nonce for authentication. Specifically, this type of authentication would be unnecessary with the Leon1 system. This is further evidenced by the fact that all of the numbers used in the bar code of Leon1 are not unique and cannot be considered to be nonces. (See e.g., Table 3 of Leon1 and arguments above).

Leon2 similarly uses a completely different type of authentication than Applicants' claimed invention. Unlike Applicants' method and nonce stamp, which can be authenticated solely using the data contained in the nonce stamp, Leon2 uses an external database or system to authenticate a stamp. In Leon2, a list of all valid serial numbers associated with labels is stored in a postage vendor system (PVS) 102. (Leon2 at par. [0124]). When a label is received from a user, its serial number is compared to the list in the PVS 102 to determine whether it is valid or invalid. After all serial numbers on a particular sheet of labels are received, the corresponding serial number is invalidated within the PVS 102. (Leon2 at par. [0130]). Because Leon2 relies on an external store or list of currently valid serial numbers to determine whether a particular serial number is valid, there would be no suggestion, motivation, or need to generate a digital signature from one of the disclosed serial numbers, to decode the digital signature, and to compare it to the serial number to determine if the

postage is valid. Rather, in Leon2, a user looks at the serial number and communicates with an external system (PVS 102) to compare it to the list of valid numbers.

Because neither of these references teaches Applicants' unique method using a nonce and a digital certificate securely derived from the nonce, they cannot obviate Applicants' method of independent claim 1 (or any claims depending claim 1, e.g., claims 8-13). Furthermore, these references teach away from Applicants' unique method of authentication, which allows users to generate postage by way of a conventional printing device, and there is no motivation or suggestion to combine the two references in the manner suggested by the Examiner. Therefore, it is respectfully asserted that this rejection has been overcome.

Moreover, Applicants' claimed invention has significant advantages over both the Leon1 and Leon2 methods of postage authentication. First, Applicants' invention allows any user to easily generate a postage indicium for their own mail piece in a secure and fraud-proof manner with a conventional printing device. Second, there is no need to continuously maintain, reference and update a data store, as taught by Leon2. Such an external data store would have to be continuously and repeatedly updated in order to ensure that the data is current. Additionally, comparing serial numbers against a very large list or store is extremely time consuming, costly and inefficient.

Both Leon1 and Leon2 use completely different methods of authenticating postage that are unrelated to and less efficient than Applicants' claimed method of independent claim 1 and dependent claims 8-13. Furthermore, there is no need, suggestion or motivation to combine the two references in the manner suggested by the Examiner. For at least these reasons, Applicants respectively request that this rejection be withdrawn.

CONCLUSIONS

For at least the reasons set forth herein, Applicants respectfully assert that all of claims 1-22 are in condition for allowance. The Examiner's early reconsideration is respectfully requested. If the Examiner has any questions, the Examiner is invited to contact Applicants' attorney at the following address or telephone number:

David Alberti
c/o Patent Department
GRAY CARY WARE & FREIDENRICH LLP
2000 University Avenue
East Palo Alto, CA 94303-2248
Telephone: (650) 833-2052

Respectfully submitted,

Gray Cary Ware & Freidenrich LLP

Dated: May 10, 2004

David Alberti
Reg. No. 43,465